California Health Benefit Exchange

CalHEERS IT Security Requirements

Review Briefing

May 2012

Table of Contents

1. Overview

CalHEERS Security and Privacy (S&P) is:

- ❑Aligned Medicaid Information Technology Architecture (MITA) 2.0 S&P guidance

- ❑Security and Privacy integration at all levels
  - ➢Business, Information and Technology architecture;
  - ➢Infrastructure Architecture, Facilities;
  - ➢Process: Service Lifecycle, Operational Processes.

- ❑Flexible and Agile S&P framework
  - ➢Open Standards Based;
  - ➢Centralized Security Policy – Implementation, Management and Monitoring;
  - ➢Consistency Across Medicaid;
  - ➢Adaptable/Responsive;
  - ➢Platform/Software Independent;
  - ➢Cross-Agency Integration and Alignment.

CalHEERS IT Security Requirements

Information about CalHEERS RFP:

- Identified 46 Security Requirements
- Covered Federal and State regulation, policy and best practices
- Called for encryption, retention and storage requirements
- Required adoption of Identity, Credential, and Access Management
- Set the security standards that the solution must meet.

CalHEERS IT Security Requirements

1. CalHEERS security requirements

EXAMPLE: CalHEERS Security and Privacy Framework shall comply, at a minimum, with the following 10 regulations/security and privacy policies:

1. Federal Information Security Management Act (FISMA) of 2002
2. Health Insurance Portability and Accountability Act (HIPAA)
3. Health Information Technology for Economic and Clinical Health Act of 1996
4. Privacy Act of 1974
5. Patient Protection and Affordable Care Act (ACA) of 2010, Section 1561
6. Safeguarding and Protecting Tax Returns and Return Information
7. E-Government Act of 2002
8. National Institution of Standards & Technology (NIST) Special Publications.
9. National Security Agency (NSA) Security Recommendation Guides
10. California Department of Health Care Services (DHCS) – Information Technology Projects Security Requirements 1 (SR1)

TR-118

CalHEERS IT Security Requirements

EXAMPLE: The CalHEERS Security and Privacy Framework shall adopt the following privacy principle in guidance with DHHS :

1. Individual Access
2. Correction
3. Openness and Transparency
4. Individual Choice
5. Collection
6. Use and Disclosure Limitation
7. Data Integrity
8. Accountability

Requirement TR-161

CalHEERS IT Security Requirements

2. Federal Security Standards

CalHEERS Security and Privacy Requirements express the need forthe following key Standards and Guidance.

- ❑ Federal Information Processing Standards Publication (FIPS PUB)
  - 199
  - 200
- ❑NIST Special Publication
  - 800-60 Volume II Revision 1
  - 800-53 Revision 3
- ❑California DHCS ISO Information Technology Project
  - Security Requirements 1 (SR1) November 2011
- ❑CMS Information Security (IS) Acceptable Risk Safeguards (ARS)
- ❑CMS System Security and e-Authentication Assurance Levels by Information Type

Assessment

3. Assessment